UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ANDREW LEONARD, NICHOLAS DEGRASSE, JAMES FRAZIER, AND CHARLES FRYE, individually and on behalf of all others similarly situated, Plaintiffs, v. MCMENAMINS, INC., Defendant.	No. 2:22-cv-00094-BJR ORDER DENYING DEFENDANT'S MOTION TO DISMISS

I. INTRODUCTION

Plaintiffs Andrew Leonard, Nicholas deGrasse, James Frazier, and Charles Frye ("Plaintiffs") bring this putative class action against Defendant McMenamins, Inc. ("Defendant" or "McMenamins"), asserting various causes of action arising from a data breach McMenamins experienced in December 2021. Presently before the Court is Defendant's motion to dismiss Plaintiffs' Amended Complaint ("Motion" or "Mot.," Dkt. 19) pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure. Plaintiffs oppose the Motion. Having reviewed the pleadings, the record of the case, and the relevant legal authorities, the Court DENIES the Motion. The Court's reasoning is set forth below.

II. BACKGROUND[1]

A. Factual Background

Plaintiffs' allegations relevant to the present motion are straightforward. On December 30, 2021, McMenamins[2] posted a notice on its website announcing that, on December 12, 2021, it had suffered a ransomware attack in which cybercriminals "installed malicious software on the company's computer systems" that temporarily prevented the company from accessing the information contained in those systems. *Id.* ¶ 29. According to the notice, the attack also enabled the hackers to steal the company's human resources and payroll data files, which contained a variety of personally identifiable information ("PII") belonging to past and present employees. *Id.* The compromised PII included the following information: "name, address, telephone number, email address, date of birth, race, ethnicity, gender, disability status, medical notes, performance and disciplinary notes, Social Security number, health insurance plan election, income amount, and retirement contribution amounts." *Id.*

Plaintiffs are current and former employees of McMenamins who provided the company with PII as a condition of their employment. AC ¶¶ 8, 12, 16, 20.[3] In January 2020, deGrasse detected several unauthorized charges to his credit card account. *Id.* ¶ 14. Although deGrasse's credit card company ultimately never billed him for those fraudulent charges, he spent approximately one-and-a-half hours disputing them and activating a new credit card. *Id.*

[1] The facts recited below are taken from Plaintiffs' Amended Complaint ("AC," Dkt. 18). For the purposes of the present motion, the Court takes the factual allegations in the Amended Complaint as true.

[2] McMenamins owns a chain of brewpubs, breweries, music venues, historic hotels, and theater pubs in Oregon and Washington, employing tens of thousands of people throughout those states. AC ¶ 28.

[3] Leonard, deGrasse, and Frazier are former employees (AC ¶¶ 8, 12, 16), and Frye is a current employee (*id.* ¶ 20).

B. Procedural Background

On August 9, 2021, Leonard filed this lawsuit as a class action "on behalf of individuals employed by McMenamins between January 1, 1998 and December 12, 2021 who had their sensitive PII accessed by unauthorized parties due to inadequate network security in a ransomware attack on McMenamins' IT systems on or around December 12, 2021." Dkt. 1 ¶ 2. In the Amended Complaint, which adds deGrasse, Frazier, and Frye as plaintiffs, Plaintiffs assert numerous causes of action arising from what Plaintiffs allege was Defendant's failure to maintain adequate network security measures as necessary to protect Plaintiffs' PII. *See generally* AC. Specifically, Plaintiffs assert claims for (1) negligence, (2) breach of contract, (3) breach of implied contract, (4) unjust enrichment, (5) breach of fiduciary duty, (6) breach of confidence, (7) bailment, (8) violation of the Washington Consumer Protection Act ("CPA"), RCW § 19.86 *et seq*., and (9) declaratory relief. AC ¶¶ 130-234. On May 27, 2022, Defendant moved to dismiss the Amended Complaint on the ground that Plaintiffs lack Article III standing to assert their claims. Plaintiffs opposed the Motion ("Opposition" or "Opp.," Dkt. 20), and Defendant replied ("Reply" or "Rep.," Dkt. 23).

III. LEGAL STANDARD

"[T]hose who seek to invoke the jurisdiction of the federal courts must satisfy the threshold requirement imposed by Article III of the Constitution by alleging an actual case or controversy." *City of Los Angeles v. Lyons*, 461 U.S. 95, 101 (1983). "[T]o satisfy Article III's standing requirements, a plaintiff must show (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Friends of the Earth, Inc.*

v. Laidlaw Env't Servs., Inc., 528 U.S. 167, 180-81 (2000) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). "The party invoking federal jurisdiction bears the burden of establishing standing." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 411-12 (2013)).

IV. DISCUSSION

Plaintiffs' claims seek two types of relief: (1) retrospective damages resulting from the theft of their PII, and (2) prospective injunctive relief requiring Defendant to strengthen its data security systems and procedures.[4] Defendant contends that Plaintiffs lack Article III standing to assert either type of claim. *See* Mot. at 5-12. The Court reviews Defendant's arguments in turn.

A. Whether Plaintiffs Have Standing to Assert Their Damages Claims

In the Motion, Defendant contends that Plaintiffs lack standing to assert their claims for damages because the harm they allege – the threatened misuse of their PII resulting from the data breach – is too "speculative" and "hypothetical" to constitute an injury-in-fact. *See* Mot. at 5-11. Plaintiffs, in response, point to three separate harms they contend constitute injuries-in-fact: (1) the "increased risk" of identity theft resulting from the data breach, "requiring them to take mitigatory action they otherwise would not have to take" (*see* Opp. at 8-12); (2) "the diminution in value of the Private Information belonging to Plaintiffs and the Class that remains in the possession and control of Defendant" (*see id.* at 12); and (3) the "actual misuse" of deGrasse's PII by cybercriminals (*see id*. at 5, 11).

[4] Specifically, Plaintiffs seek damages as part of their claims for unjust enrichment, breach of fiduciary duty, breach of confidence, and bailment (AC ¶¶ 187, 195, 206, 214); injunctive relief as part of their claim for declaratory relief (*id.* ¶ 227); and both damages and injunctive relief as part of their claims for negligence, breach of contract, breach of implied contract, and violation of the CPA (*id.* ¶¶ 147-48, 158, 178-179, 223).

The Court begins with Plaintiffs' allegations as to the increased risk of identity theft created by the data breach. Plaintiffs argue that there is a "vast body of controlling Ninth Circuit precedent" that supports standing based on such allegations. *See* Opp. at 5-6. Plaintiffs point specifically to *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) and *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018). In *Krottner*, which involved the theft of a laptop from Starbucks containing its employees' unencrypted personal information, the Ninth Circuit held that the plaintiffs' "increased risk of future identity theft" constituted a "credible threat of real and immediate harm" that sufficed to establish an injury-in-fact. *Krottner*, 628 F.3d at 1142-43. In *Zappos.com*, which involved a data breach suffered by an online retailer, the Ninth Circuit found, given the sensitivity of the stolen customer PII and indications that hackers had attempted to use it, that the plaintiffs had "alleged an injury in fact based on a substantial risk that the [] hackers will commit identity fraud." *In re Zappos.com*, 888 F.3d at 1028-29. The parties dispute whether Plaintiffs' allegations are sufficient to establish an injury-in-fact under *Krottner* and *Zappos.com* given the specific facts of those cases. *See, e.g.*, Opp. at 5-7; Rep. at 7-8. This Court, however, need not take a position on the applicability of those cases because the theory Plaintiffs draw from them – that the threat of identity theft posed by a data breach, without more, can constitute an injury-in-fact – is no longer viable under the Supreme Court's more recent decision in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

In *TransUnion*, the Supreme Court reviewed whether two classes of plaintiffs had alleged a "concrete harm" sufficient to confer standing to assert a damages claim against a credit reporting agency, TransUnion, for including false information in their credit files. *TransUnion*, 141 S. Ct.

at 2201-02.[5] The first class included plaintiffs whose reports had been disseminated to third-party businesses, while the second class included plaintiffs whose reports had not been so disseminated. *Id.* at 2208-09. In reviewing whether the plaintiffs had alleged a concrete harm, the court reasoned that, "[c]entral to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *Id.* at 2200. The court further explained that, while the most obvious concrete injuries are "traditional tangible harms, such as physical harms and monetary harms," concrete injuries can also include "intangible harms" such as "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.* at 2204. With these principles in mind, the court held that the first class's members had alleged a concrete injury because the harm they suffered – the dissemination of inaccurate credit reports to third-party creditors – bore "a 'close relationship' to the harm associated with the tort of defamation." *Id.* at 2209.

The court, on the other hand, found that the second class's members had not alleged a concrete harm. Given that those plaintiffs' inaccurate credit files were never disseminated, they "advance[d] a separate argument based on an asserted *risk of future harm*." *Id.* at 2210 (emphasis in original). Specifically, they argued that "the existence of misleading OFAC alerts in their internal credit files exposed them to a material risk that the information would be disseminated in the future to third parties and thereby cause them harm." *Id.* The court rejected the argument, finding "persuasive" the defendant's argument that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm – at least unless the exposure to the risk

[5] Specifically, the plaintiffs claimed that TransUnion violated the Fair Credit Reporting Act by including alerts in their credit files incorrectly indicating that they were on the Treasury Department's Office of Foreign Assets Control ("OFAC") list of terrorists, drug traffickers, and other serious criminals. *TransUnion*, 141 S. Ct. at 2201-02.

of future harm itself causes a *separate* concrete harm." *Id.* at 2210-11 (emphasis in original). The court reasoned, in relevant part:

> Here, the [] plaintiffs did not demonstrate that the risk of future harm materialized – that is, that the inaccurate OFAC alerts in their internal TransUnion credit files were ever provided to third parties or caused a denial of credit. Nor did those plaintiffs present evidence that the class members were independently harmed by their exposure to the risk itself – that is, that they suffered some other injury (such as an emotional injury) from the mere risk that their credit reports would be provided to third-party businesses. Therefore, the [] plaintiffs' argument for standing for their damages claims based on an asserted risk of future harm is unavailing.

Id. at 2211.

This Court, applying *TransUnion*, rejects Plaintiffs' argument that their increased risk of identity theft constitutes an injury-in-fact. *See I.C. v. Zynga, Inc.*, No. 20-cv-01539, 2022 WL 2252636, at *11 n.15 (N.D. Cal. Apr. 29, 2022) ("[I]n light of *TransUnion*'s rejection of risk of harm as a basis for standing for damages claims, the Court questions the viability of *Krottner* and *Zappos*'s holdings finding standing on this very basis."). As with the second class in *TransUnion*, Plaintiffs do not adequately allege that the risk of identity theft has materialized in any respect. While Plaintiffs allege that unauthorized charges were placed on deGrasse's credit card (AC ¶ 14), it is implausible that this resulted from, or was connected to, the data breach. In particular, Plaintiffs do not allege that their credit card information was ever provided to McMenamins, that a new credit card was opened in deGrasse's name using compromised PII, or anything otherwise indicating the use or attempted use of that PII. *See, e.g., Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1036 (N.D. Cal. 2019) ("Either the facts do not trace to the data breach at all or are so common the infinite possibilities forecloses plausibility.").

Nor do Plaintiffs articulate any "independent harm" caused by their exposure to the alleged risk of identity theft. *See TransUnion*, 141 S. Ct. at 2210-11. Although Plaintiffs point to the

"time and energy" they must now expend to monitor their accounts (*see* Opp. at 8), the Supreme Court has made clear that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 416 ("If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear."). Here, in the absence of any indication that hackers have attempted to misuse Plaintiffs' PII, and given that the data breach was caused by ransomware[6] – which was allegedly intended, at least in part, simply to prevent McMenamins from accessing its computer systems (*see* AC ¶ 29) – Plaintiffs have not adequately alleged that identity theft is "certainly impending." Further, while Plaintiffs allege that they have suffered "[a]nxiety and distress resulting [from] fear of misuse of their Private Information" (*id.* ¶ 116), "[a] perfunctory allegation of emotional distress, especially one wholly incommensurate with the stimulant, is insufficient to plausibly allege constitutional standing." *Maddox v. Bank of New York Mellon Tr. Co., N.A.*, 19 F.4th 58, 66 (2d Cir. 2021).[7] As such, consistent with *TransUnion*, the increased risk of identity theft allegedly faced by Plaintiffs cannot constitute a concrete harm sufficient for standing. *See Zynga*, 2022 WL 2252636, at *9 ("[I]n light of *TransUnion*, the Court concludes that mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft."); *see also Ewing v. MED-1 Sols., LLC*, 24 F.4th 1146, 1152 (7th Cir. 2022) ("*TransUnion* makes clear that a risk of future harm, without more, is insufficiently concrete to permit standing to sue for damages in federal court.").

[6] A ransomware attack is "an attack using a malicious software designed to deny access to a computer system until a ransom is paid." *Karter v. Epiq Sys., Inc.*, No. SACV2001385, 2021 WL 4353274, at *1 (C.D. Cal. July 16, 2021).

[7] The Amended Complaint also references "[o]ut-of-pocket costs" for the "prevention, detection, recovery and remediation from identity theft or fraud." AC ¶ 116. However, the Amended Complaint does not allege that Plaintiffs have actually paid any such costs, and in all events, such costs would be insufficient for standing under *Clapper*.

Nevertheless, Plaintiffs have alleged an injury-in-fact based not on the risk of future identify fraud created by the data breach, but on the actual harm resulting from the theft of Plaintiffs' PII itself. As noted above, *TransUnion* instructs courts, in determining whether plaintiffs have suffered a concrete harm, to inquire as to whether plaintiffs allege a harm bearing "a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *TransUnion*, 141 S. Ct. at 2209. As Plaintiffs point out, *TransUnion* specifically identifies the "disclosure of private information" as such a harm that "can [] be concrete." *Id.* at 2204; *see* Opp. at 5. Indeed, the Supreme Court and the Ninth Circuit have recognized on numerous occasions that "[v]iolations of the right to privacy have long been actionable at common law." *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017); *see U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989) ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person").

The Court finds that Plaintiffs have adequately alleged a harm bearing a "close relationship" to the harm associated with the tort of "disclosure of private information." One commits that tort when he "gives publicity to a matter concerning the private life of another … if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." Restatement (Second) of Torts § 652D; *see also Purcell v. Am. Legion*, 44 F. Supp. 3d 1051, 1061 (E.D. Wash. 2014) (articulating same cause of action under Washington law). Here, Plaintiffs allege that a variety of their "highly sensitive" personal and financial information was compromised and stolen by cybercriminals in the data breach. *See supra* at 2. Each of Plaintiffs allege that he "greatly values his privacy" and "would not have given his PII to McMenamins if he had known that it was going to maintained in

McMenamins' database without adequate protection." AC ¶ 11, 15, 19, 23. While these allegations may not state a claim for disclosure of private information,[8] Plaintiffs' alleged harm need only bear a "close relationship" to the harm resulting from that privacy tort. *See TransUnion*, 141 S. Ct. at 2209 ("we do not require an exact duplicate").

Numerous courts, including the Ninth Circuit, have found allegations concerning the interference with plaintiffs' control over their personal data to be sufficient for standing on account of their injury implicating an "invasion of the historically recognized right to privacy." *See, e.g. In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 598 (9th Cir. 2020) (allegations that Facebook interfered with plaintiffs' ability to "control[] their personal information," through its data tracking and collection practices, sufficed for standing because "[p]laintiffs have sufficiently alleged a clear invasion of the historically recognized right to privacy"); *Al-Ahmed v. Twitter, Inc.*, No. 21-cv-08017, 2022 WL 1605673, at *7 (N.D. Cal. May 20, 2022) (allegations that Twitter user's information was compromised sufficed to establish an injury-in-fact because "invasion of privacy is a particularized injury sufficient to establish Article III standing"). Further, several district courts in this Circuit and others have specifically found, following *TransUnion*, that data breach allegations similar to those of Plaintiffs relates a harm sufficiently analogous to the common law tort of "disclosure of private information," as necessary to qualify as an injury-in-fact. *See, e.g., Wynne v. Audi of Am.*, No. 21-cv-08518, 2022 WL 2916341, at *5 (N.D. Cal. July 25, 2022); *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 43 (D. Ariz. 2021); *Bohnak v. Marsh & McLennan Cos., Inc*., No. 21-cv-6096, 2022 WL 158537, at *5 (S.D.N.Y. Jan. 17, 2022); *In re USAA Data Sec. Litig.*, No. 21-cv-5813, 2022 WL 3348527, at *5 (S.D.N.Y. Aug. 12, 2022).

[8] Among other things, it is arguable whether the Plaintiffs' PII has been "given publicity," and whether its disclosure to the hackers is "highly offensive to a reasonable person."

This Court, consistent with those courts and the reasoning in *TransUnion*, finds that Plaintiffs' allegations as to the theft and resulting loss of control over their PII bear a sufficiently close relationship to the type of harm protected by that tort. As such, Plaintiffs adequately allege a concrete and actual harm sufficient to plead an injury-in-fact.

Accordingly, the Court finds that Plaintiffs have standing to assert their damages claims. Given this finding, the Court declines to review the sufficiency of Plaintiffs' other alleged harms.

B. Whether Plaintiffs Have Standing to Seek Prospective Injunctive Relief

As noted above, Plaintiffs' claims for negligence, breach of contract, breach of implied contract, violation of the CPA, and declaratory relief seek, in part, prospective injunctive relief requiring Defendant to undertake various actions to safeguard the PII McMenamins currently possesses.[9] Unlike their damages claims based on the past theft of Plaintiffs' PII, the injunctive relief sought by Plaintiffs concerns continuing actions by Defendant related to its current possession of Plaintiffs' PII. Defendant argues that Plaintiffs Leonard, deGrasse, and Frazier lack standing to seek that relief because they "have failed to allege that (1) they actually will benefit from the relief they seek, and (2) the harm they seek to prevent is imminent and substantial." Mot. at 11-12.

As the Supreme Court explained in *TransUnion*, "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion*, 141 S. Ct. at 2210; *see Bates v. United Parcel Serv., Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) ("The plaintiff must

[9] For example, Plaintiffs' claims for negligence and breach of implied contact seek "injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members." AC ¶¶ 148, 179.

demonstrate that he has suffered or is threatened with a 'concrete and particularized' legal harm, coupled with 'a sufficient likelihood that he will again be wronged in a similar way.'" (citations omitted)). Further, "it must be likely that a favorable judicial decision will prevent or redress the injury." *Summers v. Earth Island Inst.*, 555 U.S. 488, 493 (2009).

Defendant contends that Leonard, deGrasse, and Frazier will not benefit from the injunction they seek because they are former employees, and "McMenamins already has strengthened its security systems." *See* Mot. at 11-12. That contention is without merit. First, there is no difference between McMenamins's current and former employees insofar as the company possesses PII belonging to both categories of employees. *See, e.g.*, *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1141 (C.D. Cal. 2021) (plaintiffs had standing to seek injunctive relief based on allegations that defendants "still possess[ed] [plaintiffs'] private information" and had not announced significant changes to their security system following data breach); *see also In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-cv-0514, 2018 WL 2128441, at *14 (N.D. Ga. Mar. 5, 2018) ("Plaintiffs allege that [company] still possesses their customer data and therefore they have an interest in ensuring its protection from further breaches.").[10] Second, Defendant's assertion that McMenamins has already strengthened its data security is unsupported and, more importantly, premature at this stage of litigation. *See Bell v. Blizzard Ent., Inc.*, No. 2:12-cv-9475, 2013 WL 12063912, at *6 (C.D. Cal. Apr. 3, 2013) (allegations that company suffered past breaches and "has made no additional effort to secure [plaintiffs'] information" were

[10] In its Reply, Defendant points to an allegation in the Amended Complaint in which Plaintiffs request "injunctive relief requiring Defendant to employ adequate security practices … to protect McMenamins's employees' PII." AC ¶ 227; *see* Rep. at 10. According to Defendant, that allegation shows that "Plaintiffs seek injunctive relief solely 'to protect McMenamins [current] employees' PII.'" Rep. at 10 (citing AC ¶ 227). Given the nature of Plaintiffs' claims and requests for injunctive relief articulated elsewhere in the Amended Complaint, the Court interprets that allegation as seeking relief on behalf of both current and former employees.

sufficient at the pleadings stage "to confer Article III standing as to their request that [company] be forced to take additional security measures"); *see also Arby's*, 2018 WL 2128441, at *14 (rejecting, as "premature," defendant's motion to dismiss argument that plaintiffs had not alleged any facts about company's "current security posture" demonstrating a risk of future breach).

Defendant's contention that Plaintiffs do not allege a risk of "imminent and substantial" harm also lacks merit. In the Motion, Defendant argues that Plaintiffs fail to adequately allege an imminent and substantial risk of identity theft resulting from hackers' misuse of the previously compromised data. *See* Mot. at 12. However, as the Opposition points out, Plaintiffs' request for injunctive relief is based on the "risk of subsequent breaches" of McMenamins's data security system that would compromise the PII that "is still in Defendant's possession and control." Opp. at 15. Defendant, in its Reply, abandons its argument. Given Plaintiffs' allegations that McMenamins has maintained inadequate data security measures to safeguard its former and current employees' PII (*see* AC ¶¶ 37-60), and that McMenamins's data security system was breached in December 2021 (*see, e.g.*, *id.* ¶ 29), the Court finds that Plaintiffs have alleged an imminent and substantial risk of harm resulting from a future breach and theft of their PII. *See Ambry Genetics*, 567 F. Supp. 3d at 1141; *Bell*, 2013 WL 12063912, at *6; *see also In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-md-2583, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016) (denying motion to dismiss claim for injunctive relief where plaintiffs alleged that "Defendant's security measures continue to be inadequate and that they will suffer substantial harm" with respect to "a future breach").

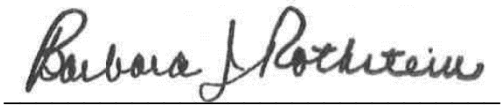
Accordingly, the Court finds that Plaintiffs have standing to pursue injunctive relief.

V. CONCLUSION

For the foregoing reasons, the Court rejects Defendant's arguments that Plaintiffs lack Article III standing to assert their claims. Therefore, Defendant McMenamins's motion to dismiss (Dkt. 19) is DENIED.

SO ORDERED.

Dated: September 2, 2022



Barbara Jacobs Rothstein
U.S. District Court Judge